

ABSTRACT

The present invention discloses a method for generating and verifying a user attestation-signature value (DAA') and issuing an attestation value (*cert*) for the generation of the user attestation-signature value (DAA'). Further, the invention is related to a system for using a user attestation-signature value (DAA') that corresponds to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one or more of the attribute values (x, y) remaining anonymous for transactions, the system comprising: a user device (20) having a security module (22) that provides a module public key (PK_{TPM}) and a security module attestation value (DAA), the user device (20) providing a user public key (PK_{UC}) that inherently comprises none, one, or more user determined attribute value (x, y) and a proof value demonstrating that the user public key (PK_{UC}) is validly derived from the module public key (PK_{TPM}) of the security module (22); an attester computer (30) that provides none, one, or more attester determined attribute value (w, z) and an attestation value (*cert*) that bases on an attester secret key (SK_{AC}), the user public key (PK_{UC}), and an anonymous attribute value (w, z); and a verification computer (40) for verifying whether or not (i) the user attestation-signature value (DAA') was validly derived from the security module attestation value (DAA) provided by the security module (22) and the attestation value (*cert*), and (ii) the attestation value (*cert*) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z).